Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Penetration Testing - Is it right for you?

The process of performing a penetration test is to verify that new and existing applications, networks and systems are not vulnerable to a security risk that could allow unauthorized access to resources. This paper will review the steps involved in preparing for and performing a penetration test. The intended audience for this paper is project directors or managers who might be considering having a penetration test performed. The process of performing a penetration test is complex. Each company must determine if the pr...

Copyright SANS Institute
Author Retains Full Rights

AD

Penetration Testing – Is it right for you?

Abstract

The process of performing a penetration test is to verify that new and existing applications, networks and systems are not vulnerable to a security risk that could allow unauthorized access to resources. This paper will review the steps involved in preparing for and performing a penetration test. The intended audience for this paper is project directors or managers who might be considering having a penetration test performed. The process of performing a penetration test is complex. Each company must determine if the process is appropriate for them.

Introduction

Over the last few years, companies have been adding additional functionality to existing applications and implementing new applications in an effort to provide more convenience or better service for customers and/or employees. Examples of this functionality could be in the form of World Wide Web access for bank customers or telecommuting options for employees who work at home. Additionally, companies have also determined that a presence on the World Wide Web is a way to increase brand awareness and establish a top-of-mind awareness for their product or service for potential customers. Security is a significant concern for World Wide Web servers. The World Wide Web servers have added a new set of vulnerabilities that companies should consider. However, vulnerabilities are not limited to World Wide Web servers. Vulnerabilities exist and can be unintentionally induced in systems or resources that have been in operation for an extended period.

What is a penetration test?

A penetration test is the authorized, scheduled and systematic process of using known vulnerabilities in an attempt to perform an intrusion into host, network or application resources. The penetration test can be conducted on internal (a building access or host security system) or external (the company connection to the Internet) resources. It normally consists of using an automated or manual toolset to test company resources.

What is a penetration test is not.

A penetration test is not an uncoordinated attempt to access an unauthorized resource. The event must be coordinated and scheduled with support staff. At a minimum, some of these tests will log alerts in an Intrusion Detection System[1]. Additionally, some tests have the ability to cause an outage of network equipment or systems. For that reason, management and staff awareness is required in most cases. The exception to complete notification could be a penetration test intended to test the Intrusion Detection System (and staff response). Management should also consider

[1] Intrusion Detection Systems consist of Network based and Host based systems that document and report events that are potential violations of the implemented security policy. Network based systems are normally used on Firewall configurations. Host based systems are normally implemented on core applications and platforms.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

providing printed documentation authorizing the test be performed. This will address any legal liabilities that might be associated with the performance of the test.

Why perform a Penetration Test?

If a vulnerability is utilized by an unauthorized individual to access company resources, company resources can be compromised. The objective of a penetration test is to address vulnerabilities before they can be utilized.

What should be tested?

The core services offered by the company should be tested. These include: Mail, DNS, firewall systems, password syntax, File Transfer Protocol (FTP) systems and Web servers. The most recent information indicates that company wireless systems and Public Branch Exchange (PBX) systems should also be tested. Companies should also test other potential methods for accessing the computing, network resources and or obtaining information. These include physical access to the computing/network and backup areas in addition to social engineering access attempts.

Preparing for the test

Prior to performing a penetration test an organization must have a Computer Security Policy. As described in http://www.ietf.org/rfc/rfc2196.txt?number=2196
"2.1.1
A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide." When writing a security policy, the value of the company's information resources and assets should take into account and appropriate security processes assigned. The cost incurred to the company if the data was lost should be the primary factor in determining the appropriate security actions and processes that make up the policy. For example, if the company deals with government information or financial records, the process of deactivating the user ID might be performed differently than at a local college. Further, if a company had proprietary information, trade secrets or even customer lists that a competitor could utilize, a higher value should be assigned to this information and appropriate security steps taken.
The Security Policy should have information about:

- The connections to/from the Internet
- Dial-up connections
- Physical security access
- Password management
- User rights and responsibilities
- Administrator rights and responsibilities
- Protection of sensitive information
- Emergency procedures
- Documentation
- Backups

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Logs
- Incident handling
- How people go about reporting a security issue
- Types of violations that should be reported
- Enforcement of the policy
- Who is ultimately responsible

A dedicated document on writing an effective security policy can be found at http://csrc.nist.gov/isptg/html/ISPTG-Contents.html

Should the penetration test use existing staff or be contracted out to a third party company?

The answer to the question could depend on what is to be tested and how much time is available.

If the test will include physical access to secured areas and or attempts to obtain information via social engineering processes, contracting an outside company to perform the test would probably obtain more accurate results. Being unassociated with the organization, an outside penetration testing company can better replicate the steps, and efforts an individual might attempt when trying to obtain access or information. Additionally, because representatives from the company will be unknown to the support staff at the organization, the results of the test will not be skewed because of any familiarity that support staff had with an individual who is performing the test.

Internal versus External penetration tests

The threat you are attempting to replicate should factor into the decision on how the test should be conducted, by whom (and to extent who should conduct the test). Tests intended to identify vulnerabilities with physical access or exposures to social engineering are referred to as **internal penetration tests**. Internal penetration tests are intended to determine what vulnerabilities exist for systems that are accessible to authorized network connections (or login Ids) that reside within the network domain of the organization. An internal test might better replicate the efforts a recently terminated employee might take when attempting to access valuable information. Conversely, **external penetration tests** are intended to identify vulnerabilities that are present for connections that have been established through the organization connection to the Internet (also known as the firewall or gateway). If the primary objective of the test is to ensure that the Payroll Database is sufficiently secure from the corporate Internet site, an external penetration test is more appropriate.

Considerations for using a penetration testing company

If a penetration testing company is to be used, some effort should be made to confirm the qualifications of the company selected. What are the qualifications and backgrounds of the employees that work for the company? As pointed out in http://www.fdic.gov/news/news/financial/1999/FIL9968a.HTML, some companies (such as financial institutions) are "under federal obligation to avoid employing people if the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

individual in question has been convicted of a felony or breach of trust that would involve more than one year in prison." Additionally, to ensure the test is proceeding as planned, the company should provide a representative on-site during the test. This will provide an opportunity to terminate the test if a problem is identified. Some tests have involved the notification of authorities because the support staff were not aware a test was in progress and there was no company representative available to intercede.

Scope of the test

Following the selection of team (be it made up of internal staff or a third party) to perform the test, the scope of the test should be determined. This will provide the testing parameters that the team will use to identify the vulnerabilities. Some issues that should be determined include:

- What is the time interval for the test?
- Who will be notified of the test?
- What will be used to confirm that unauthorized access was obtained?
- What systems/resources will be initially tested and how?
    - Firewall configuration
        - Full knowledge (also know as with information[2])
        - Zero knowledge (also known as without information)
    - Host systems
        - Web servers
            - Production or development system?
        - Password selection
        - Trusts or shares between systems
        - FTP servers
        - Intrusion Detection system
    - DNS servers
    - Dial in modems
    - Wireless access
    - Public Branch Exchange (PBX)
    - User ID deactivation or employee termination process
    - Physical access
    - Social engineering
    - Desktop computers
        - Password selection
        - Modems set for auto-answer and or remote access software
- How will the results be presented?
- When will another test be performed to confirm the results of the changes?

Gathering information on the company (discovery)

[2] There is a recent trend with third party companies who perform penetration testing. Many companies are now requesting the Access Control List of a firewall system. This is known as full knowledge or with information. The reason behind the request is the penetration test will be incomplete without the information. The rebuttal to this statement is that a hacker from the Internet will not have access to the firewall ACL. The decision to provide this information should be left up to the company that has requested the test. See closing comments for issues involved.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Following the selection of a test team and test process, research begins on the company to be tested. A number of resources and tools are available that provide initial information about a target companies systems and resources. Some resources are as simple as newsgroup posts by employees of the target company. As pointed out in http://shrike.depaul.edu/~mchen/420/natalya.html
"Newsgroup posts can not only provide some information about the employees but also the specific resource or system from where the post originated." This is kind of like just being a very astute listener at the company water fountain. Company employees often provide value pieces of information without realizing it. Other methods to gather information include: Whois, Nslookup, ping, telnet and traceroute. In many cases, these applications are installed with the operating system. In other instances, the software is publicly available on the Internet. A brief explanation of the tools is provided:

Whois – performs a Internet lookup using directory services
Nslookup - performs an interactive query to domain name servers
Ping – sends an ICMP ECHO Request to a specific network host (a port can be included in the ping. If a response it received for a specific port, it indicates that the port is open for TCP/IP communication)
Telnet – attempts to establish an interactive telnet connection to a specific host system (a port can be included in the telnet. If a response it received for a specific port, it indicates that the port is open for TCP/IP communication)
Traceroute – identifies the Internet communication paths between two systems attached via TCP/IP

Each of the tools above can provide additional information about a network connection or host system. In this initial phase of the test, having as much information as possible is preferred. It will help define the proper test to select. Additionally, because an unauthorized user will perform as much research as possible before attempting an access attempt, it is prudent that a company employee have a comparable amount of information before any further investigation is performed. The fewer network and system details that can be compiled by using the tools identified above will improve security.

Gathering information about systems (inventory scan)
The Inventory scan process involves obtaining as much information as possible about the system that is targeted for the penetration test. Information of value: Operating System (including version number) in use, applications and application versions. With the Operating System and application specific information, only the known vulnerabilities that exist for the specific Operating System and or application need be tested. This is the distinction between an indiscriminate address space probe for any open ports (also known as script kiddies) and an actual penetration test.

One of the best tools for determining Operating System is **Nmap** – (http://nmap.org).
An article on **Nmap** use can be found at http://rr.sans.org/audit/nmap2.php.

Exploitation of vulnerabilities
The exploitation phase of the penetration test is performed by using a vulnerability scanner to identify problems with the configuration of a system. There are number of

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

freeware and commercial tools that perform specific functions. The tools (subset of the tools mentioned at http://nmap.org/tools.html) include:

Nessus – (http://www.nessus.org) A network vulnerability scanner tool for Unix systems.

SARA – (http://www-arc.com/sara/) The second successor to the **SATAN** vulnerability scanner tool (first successor was **SAINT**)

Whisker – (http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2) A CGI vulnerability scanner

Hping2 – (http://www.kyuzz.org/antirez/hping/) A network tool that can send custom ICMP, UDP or TCP packets. Allows testing of firewall rules and supporting testing of fragmented packets.

Firewalk – (http://www.packetfactory.net/Projects/Firewalk/) A traceroute like tool that allows the Access Control Lists of a firewall to be determined and a network map can be created.

John The Ripper – (http://www.openwall.com/john/) John is an active password cracking tool to identify weak password syntax.

Crack / Libcrack – (http://www.users.dircon.co.uk/~crypto/) A password cracking tool for Unix systems.

NAT (NetBIOS Auditing tool) – (http://www.tux.org/pub/security/secnet/tools/nat10/) A tool to identify vulnerabilities in a NetBIOS configuration of a **NT** system.

Toneloc – A war dialer to check for modems on desktop systems that are set for auto-answer and or run remote access software.

Commercial products (from http://nmap.org/tools.html and http://www.timberlinetechnologies.com/products/vulnerability.html)

Internet Security Server – (http://www.iss.net) ISS is probably the top commercial product. Many penetration testing companies use ISS and CyberCop

CyberCop – (http://www.pgp.com/asp_set/products/tns/ccscanner_intro.asp) A popular commercial vulnerability scanner.

L0pht Crack – (http://www.l0pht.com/l0phtcrack/) A **NT** password cracking tool. Employs brute force, hybrid and dictionary tests for guessing passwords.

Phonesweep – (http://www.sandstorm.net/) – A war dialer to check for modems on desktop systems that are set for auto-answer and or run remote access software.

Also included at http://nmap.org/tools.html is a list of products for performing Intrusion Detection. There are also tools that help manage the volume of data that is created in the intrusion detection process. Intrusion detection is outside the topic of this paper (but is related to penetration testing) and those products were not included for that reason.

Following the selection of a vulnerability assessment tool, it should be used on a system or network identified as the initial target.

The information provided by the most advanced tools (like **Nessus**) clearly indicates the major vulnerabilities. Following the determination of a possible vulnerability, a process

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

or task should be performed confirms the existence of the vulnerability. The process might involve placing a file in the directory area that was intended to be controlled access, changing the password on a guest logon ID, or renaming a file on a test server that was thought to be inaccessible. In the case of a physical access penetration test it might involve obtaining a piece of documentation from the computer room. Or finding out a home phone number of a systems manager in the case of a social engineering test.

Providing the results of the Test

The results of the test should include solutions to reduce or eliminate the vulnerabilities. This is what differentiates a penetration test and a security audit. The significant vulnerabilities identified should be addressed first and a schedule determined to verify that the vulnerabilities have been addressed. The next department, network or system can then be selected for the same penetration testing process (or a slightly revised one if there are differences in the system configuration).

The solutions implemented will be dependant on the vulnerabilities identified, the loss to the company if conditions triggering the vulnerability occurred, and the cost (and effectiveness) of the available solutions. One solution might require that a new system running a web server must pass a vulnerability test before the web port is opened at the firewall. Another solution might require that all mail within the domain is sent to a central mail system and delivered to local host systems by the central mail server.

Enforcement of the existing policy might be the only condition required to address certain vulnerabilities. In the case of desktop security, remote administration software might be already prohibited at the company. But a better job needs to be done to ensure compliance. There will also be vulnerabilities that can be addressed by applying the most recent version of the application or operating system patch.

The results of the report should be closely guarded. If the information fell into the wrong hands, an unauthorized individual could exploit the recently identified vulnerabilities before the vulnerabilities have been addressed.

Test limitations

Penetration test is just a snapshot of the systems and networks at a specific time. The test was only performed on the vulnerabilities that were known by the various tools or packages and on the systems accessible at that time. The process of application, system and network security is a continuous one because as soon as the test is complete, another system or application could be added to the business that might produce different results if the test were again performed.

Company and test considerations

The process of performing a penetration test (prevention) is important but detection is imperative. An intrusion detection system (or multiple IDS applications in various places) is required.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

If the penetration test is intended to test the functionality of an intrusion detection system (and staff response), a slightly different process is needed. Some support staff cannot be made aware of the pending test. However, their actions must be monitored to ensure that they do not make a decision based on the assumption that the event is a legitimate attack. This includes the possibility of notifying authorities or performing extensive-labor intensive research into the cause of the condition.

If a test the intrusion detection system is involved, a false sense of security could be created. An attempt to access company data by an unauthorized individual would probably be conducted over a longer period of time and possibly would not cause IDS to reach the thresholds that were experienced during the penetration test. This is one of the reasons a Host based intrusion detection system should also be used. A host based IDS can provide an extra safeguard on the alteration of files or configurations. Packages like **Tripwire** can be very valuable and cost effective. For the threat of a recently terminated employee accessing valuable data, host based systems should always be utilized.

If a company decided to use a third party to perform an external penetration test, some research should be performed into what tools will be used. A quote from http://www.ideahamster.org/osstmm.htm provides the example that "while many companies say their tools consist of **ISS**, **CyberCop** and proprietary in-house developed tools, this really means just **ISS** and **CyberCop**." Additionally, as stated in the **March 1998** issue of the **Computer Security Institute's *Alert*** magazine, "Some teams use homegrown tools kits. Teams that build their own tool kits, rather than relaying on commercial products like ISS, seem to have a greater understanding of the underlying issues. After all, **ISS** is built and marketed for organizations to use themselves, why pay consultants to come in and use it for you?"

Depending on the third party company selected, the company could request the firewall Access Control List (ACL) and network map. There does not appear much agreement over the need for this information (also known as full knowledge versus zero knowledge). Since it would not be available to a hacker, why should it be made available to the company? However, due to the time constraints associated with a penetration test performed by a third party, (which would not be a factor for a event involving a hacker), providing the information will result in a more complete test and that is the real objective.

Some closing comments

One area that was not discussed in the previous text was a penetration test for a Denial of Service (**DoS**) attack. The consensus now appears to be that there really is no way to prevent them. Any penetration test that includes a **DoS** attack will be successful. For a **DoS** attack, there is no solution that will eliminate the risk. For that reason, they were not considered as a vulnerability that has a solution and were not included in the text.

The objective of this paper was not to convenience someone to perform a penetration test. The objective was to help provide some details about what is involved with having a test performed, issues to be considered and what should be the results of the test. Because the company's Security Policy and the use of Intrusion Detection Software play a very

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

important role in the impact of performing a penetration test and the success at implementing long-term solutions, a penetration test is a very complex process that has implications company wide. The decision to perform a penetration test should be made on a company-by-company and condition-by-condition basis.

References

1. Fraser, B "Site Security Handbook" September 1997 URL http://www.ietf.org/rfc/rfc2196.txt?number=2196

2. Herzog, Pete "THE OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL" May 25, 2001 URL http://www.ideahamster.org/osstmm.htm

3. Kaye, Krysta "Vulnerability Assessment of a University Computing Environment" May 28, 2001 URL http://rr.sans.org/casestudies/univ_comp.php

4. N/A "Risk Assessment Tools and Practices for Information System Security" URL http://www.fdic.gov/news/news/financial/1999/FIL9968a.HTML

5. Klikushina, Natalya "Firewall Penetration" URL http://shrike.depaul.edu/~mchen/420/natalya.html

6. N/A "Nmap Free Stealth Security Scanner" URL http://nmap.org

7. Corcoran, Tim "An Introduction to NMAP" Oct 25, 2001 URL http://rr.sans.org/audit/nmap2.php

8. N/A "Quality Security Tools" URL http://nmap.org/tools.html

9. N/A "Internet Security Systems" URL http://www.iss.net

10. Kurtz, George and Prosise, Chris "Security Strategies" Information Security Magazine September 00
(also available at URL http://www.infosecuritymag.com/articles/september00/features3.shtml)

11. Antionline.com - http://www.antionline.com/index.php?action=forums

12. Moyer, Philip "Penetration Testing: Issues for Management". Computer Security Institute's Alert Magazine March 1998
(also available at URL http://www.gocsi.com/penet.htm)

13. McClure, Stuart; Scambray, Joel; Kurtz, George Hacking Exposed Berkley, Osborne 1999

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**